

(12) DEMANDE INTERNATIONALE PUBLÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international(43) Date de la publication internationale  
29 janvier 2004 (29.01.2004)

PCT

(10) Numéro de publication internationale  
WO 2004/010642 A1(51) Classification internationale des brevets<sup>7</sup> : H04L 9/32(21) Numéro de la demande internationale :  
PCT/FR2003/002251

(22) Date de dépôt international : 16 juillet 2003 (16.07.2003)

(25) Langue de dépôt : français

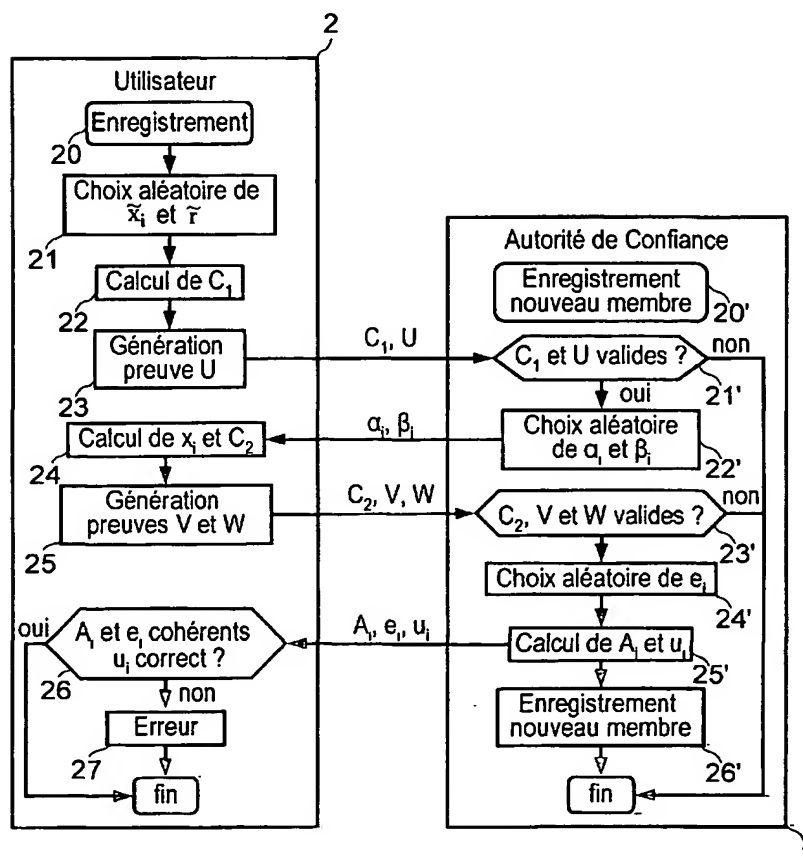
(26) Langue de publication : français

(30) Données relatives à la priorité :  
02/09218 19 juillet 2002 (19.07.2002) FR(71) Déposant (pour tous les États désignés sauf US) :  
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,  
F-75015 Paris (FR).(72) Inventeurs; et  
(75) Inventeurs/Déposants (pour US seulement) : CANARD,  
Sébastien [FR/FR]; 4, résidence Olympia, F-14000 Caen  
(FR). GIRAULT, Marc [FR/FR]; 4, rue Viviane, F-14000  
Caen (FR). TRAORE, Jacques [FR/FR]; 23, avenue de la  
Suisse Normande, F-61100 Saint Georges des Groseillers  
(FR).

[Suite sur la page suivante]

(54) Title: LIST SIGNATURE METHOD AND APPLICATION TO ELECTRONIC VOTING

(54) Titre : PROCEDE DE SIGNATURE DE LISTE ET APPLICATION AU VOTE ELECTRONIQUE



(57) Abstract: The invention concerns a list signature method comprising: an organization phase whereby reliable authority defines parameters for implementing an anonymous electronic signature; a phase which consists in registering persons on a list of authorized members to generate a list signature, during which each person calculates a private key, and the reliable authority delivers to each person a certificate for membership of the list; a phase which consists in defining a serial number; a phase wherein a member of the list generates by means of certificate a signature containing an element common to all the signatures issued by one single member with one single serial number; a phase which consists in verifying whether the signature has been generated by a member of the list and whether the serial number has been used to generate the signature.

(57) Abrégé : Le procédé de signature de liste comprend : une phase d'organisation consistant pour une autorité de confiance à définir des paramètres de mise en oeuvre d'une signature électronique anonyme ; une phase d'enregistrement de personnes dans une liste de membres autorisés à générer une signature de liste, durant

laquelle

[Suite sur la page suivante]

WO 2004/010642 A1



(74) Mandataires : DE ROQUEMAUREL, Bruno etc.; Novagraaf Technologies, 122, rue Edouard Vaillant, F-92593 Levallois Perret Cedex (FR).

(81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

---

chaque personne calcule une clé privée, et l'autorité de confiance délivre à chaque personne un certificat de membre de la liste ; une phase de définition d'un numéro de séquence ; une phase de génération par un membre de la liste à l'aide de son certificat d'une signature contenant un élément commun à toutes les signatures émises par un même membre avec un même numéro de séquence ; une phase de vérification de signature consistant à vérifier que la signature a été générée par un membre de la liste et que le numéro de séquence a été utilisé pour générer la signature.

PROCEDE DE SIGNATURE DE LISTE ET APPLICATION AU VOTE ELECTRONIQUE.

5 La présente invention concerne le domaine général de la sécurité des services accessible par un réseau de transmission de données numériques, et plus précisément le domaine de la signature électronique.

Elle s'applique notamment, mais non exclusivement au vote électronique ou  
10 encore à la pétition électronique.

La signature électronique d'un message met en œuvre un mécanisme relevant de la cryptographie dite à clé publique : le signataire qui possède une clé secrète ou privée et une clé publique associée, peut produire une signature de message à  
15 l'aide de la clé secrète. Pour vérifier la signature, il suffit de disposer de la clé publique.

Dans certaines applications comme le vote électronique, le signataire doit pouvoir rester anonyme. A cet effet, on a mis au point ce que l'on appelle la  
20 signature électronique anonyme permettant à l'aide d'une clé publique de déterminer si le signataire d'un message possède certains droits (droit de signer le message, droit de posséder la clé secrète ayant été utilisée pour signer le message, etc.), tout en préservant l'anonymat du signataire. En outre, dans les applications de vote ou de pétition électronique, chaque personne autorisée ne  
25 doit pouvoir signer qu'une seule fois.

Parmi les signatures anonymes, il existe également ce que l'on appelle la signature aveugle permettant à une personne d'obtenir la signature d'un message d'une autre entité, sans que celle-ci ait à connaître le contenu du  
30 message et puisse établir plus tard le lien entre la signature et l'identité du signataire. Cette solution de signature aveugle nécessite donc l'intervention d'une entité intermédiaire qui produit les signatures. Dans les applications comme le vote ou la pétition électronique, cette solution fait intervenir une autorité habilitée qui signe le vote de chaque électeur ou la pétition pour chaque  
35 pétitionnaire.

On a également proposé le concept de signature de groupe qui permet à chaque membre d'un groupe de produire une signature telle qu'un vérificateur

possédant une clé publique adéquate peut vérifier que la signature a été émise par un membre du groupe sans pouvoir déterminer l'identité du signataire.

Ce concept est par exemple décrit dans le document :

- [1] "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme" de G. Ateniese, J. Camenisch, M. Joye et G. Tsudik, in M. Bellare, Editor, *Advance in Cryptology – CRYPTO 2000*, vol. 1880 of LNCS, p. 255-270, Springer-Verlag 2000.

Cependant, dans ce concept, une autorité de confiance peut lever à tout moment cet anonymat et déterminer l'identité d'une personne du groupe ayant émis une signature. En outre, ce type de signature est dit "non fiable", c'est-à-dire qu'il ne permet pas de déterminer si oui ou non deux signatures ont été émises par la même personne sans lever l'anonymat de la signature. Les signatures de groupe sont utilisées dans de nombreuses applications, telles que la vente aux enchères électronique, la monnaie électronique ou encore le vote électronique. La signature de groupe ne convient pas parfaitement à cette dernière application puisqu'elle autorise une autorité de confiance à accéder à l'identité d'un signataire, et ne permet pas de relier deux signatures émises par une même personne sans déterminer l'identité du signataire. En outre, le document [1] ne prévoit pas de processus de révocation d'un membre du groupe.

Pour remédier à ce dernier inconvénient, le document [2] "Efficient Revocation of Anonymous Group membership Certificates and Anonymous Credentials" de J. Camenisch et A. Lysysanskaya, publié par Cryptologie ePrint Archive IACR. 2002, prévoit d'ajouter à ce concept un processus de révocation (ce document sera aussi publié par M. Jung, Editor *CRYPTO 2002*, Springer-Verlag 2002). Toutefois, cette solution n'apporte pas de solution aux problèmes de la préservation de l'anonymat du signataire et de "fiabilité" de deux signatures.

Dans une application de vote électronique, il est en outre nécessaire pour assurer une sécurité se rapprochant au maximum du vote traditionnel, de garantir les propriétés suivantes.

Nul ne doit être capable de connaître même partiellement les résultats du scrutin avant sa clôture. Tout le monde doit pouvoir se convaincre de la validité du résultat final du scrutin. Enfin, une autorité habilitée doit être capable de retirer ou de révoquer le droit de vote d'une personne.

Qu'il s'agisse du vote hors ligne, c'est-à-dire de l'utilisation d'une machine à voter électronique installée dans un bureau de vote, ou du vote en ligne, c'est-à-

dire à distance, via le réseau Internet par exemple, les systèmes proposés actuellement, utilisant une signature de groupe telle que décrite dans le document [1] et complétée dans le document [2], ne remplissent pas ces conditions, mis à part la révocation du droit de signature.

5

Par ailleurs, l'application du concept de signature aveugle au vote électronique est une solution dont la mise en œuvre est lourde, car elle oblige l'électeur à se connecter plusieurs fois à chaque élection. En outre, si le scrutin se passe mal, on ne peut pas déterminer qui en est le responsable : un électeur ou  
10 l'organisateur du scrutin.

On a également proposé, notamment dans le document [3] "Untraceable Electronic Mail Return Addresses and Digital Pseudonym" de D. Chaum, ACM 1981, le concept de réseaux mélangeurs, chaque mélangeur étant une fonction  
15 produisant une liste de nombres déchiffrés à partir d'une liste de nombres chiffrés, tout en cachant la correspondance entre les nombres chiffrés et les nombres déchiffrés. Appliquée au vote électronique, cette technique présente l'inconvénient majeur de ne pas permettre de vérifier la validité d'un vote sans compromettre le secret de celui-ci.

20 Dans le document [4] "A Secure and Optimal Efficient Multi-Authority Election Scheme", de Cramer, Gennaro, et Schoenmakers, Eurocrypt'97, LNCS – Springer-Verlag, il est décrit ce que l'on appelle le chiffrement homomorphe permettant d'effectuer des calculs de base sur des nombres chiffrés. Les solutions basées sur ce procédé ne sont cependant pas applicables aux scrutins  
25 impliquant un grand nombre d'électeurs.

La présente invention a pour but de supprimer cet inconvénient. Cet objectif est atteint par la prévision d'un procédé de signature de liste comprenant au moins :

- 30 – une phase d'organisation consistant pour une autorité de confiance à définir des paramètres de mise en œuvre d'une signature électronique anonyme, dont une clé privée et une clé publique correspondante,
- une phase d'enregistrement de personnes dans une liste de membres autorisés à générer une signature électronique propre aux membres de la liste, au cours  
35 de laquelle chaque personne à enregistrer calcule une clé privée à l'aide de paramètres fournis par l'autorité de confiance et de paramètres choisis aléatoirement par la personne à enregistrer, et l'autorité de confiance délivre à chaque personne à enregistrer un certificat de membre de la liste,

- une phase de signature au cours de laquelle un membre de la liste génère et émet une signature propre aux membres de la liste, cette signature étant construite de manière à contenir une preuve que le membre de la liste ayant émis la signature, connaît un certificat de membre de la liste, et
  - 5 - une phase de vérification de la signature émise comprenant des étapes d'application d'un algorithme prédéfini pour mettre en évidence la preuve que la signature a été émise par une personne en possession d'un certificat de membre de la liste.
- 10 Selon l'invention, ce procédé comprend en outre :
- une phase de définition d'une séquence consistant pour l'autorité de confiance à générer un numéro de séquence à utiliser dans la phase de signature, une signature générée durant la phase de signature comprenant un
  - 15 élément de signature qui est commun à toutes les signatures émises par un même membre de la liste avec un même numéro de séquence et qui contient une preuve que le numéro de séquence a été utilisé pour générer la signature, la phase de vérification comprenant en outre une étape de vérification de la preuve que le numéro de séquence a été utilisé pour générer la signature;
  - 20 - une phase de révocation d'un membre de la liste pour retirer un membre de la liste, au cours de laquelle l'autorité de confiance retire de la liste le membre à retirer et met à jour les paramètres de mise en œuvre de la signature électronique anonyme, pour tenir compte du retrait du membre de la liste; et
  - une phase de mise à jour des certificats des membres de la liste pour tenir
  - 25 compte de modifications de la composition de la liste.

Selon un mode de réalisation de l'invention, la phase d'organisation comprend la définition d'un paramètre commun dépendant de la composition de la liste, la phase d'enregistrement d'une personne dans la liste comprenant la définition

30 d'un paramètre propre à la personne à enregistrer qui est calculé en fonction du paramètre dépendant de la composition de la liste et qui est intégré au certificat remis à la personne, la phase d'enregistrement comprenant une étape de mise à jour du paramètre commun dépendant de la composition de la liste, la phase de révocation d'un membre de la liste comprenant une étape de modification du

35 paramètre commun dépendant de la composition de la liste, pour tenir compte du retrait du membre de la liste, et la phase de mise à jour des certificats des membres de la liste comportant une étape de mise à jour du paramètre propre à chaque membre de la liste pour tenir compte des modifications de la

composition de la liste.

Selon un mode de réalisation de l'invention, une signature propre à un membre de la liste et possédant le certificat  $[A_i, e_i]$  comprend des paramètres  $T_1, T_2, T_3$

5 tels que :

$$T_1 = A_i b^\omega \pmod{n},$$

$$T_2 = g^\omega \pmod{n},$$

$$T_3 = g e_i h^\omega \pmod{n},$$

10  $\omega$  étant un nombre choisi aléatoirement lors de la phase de signature, et  $b, g, h$  et  $n$  étant des paramètres généraux de mise en œuvre de la signature de groupe, tels que les paramètres  $b, g$  et  $h$  ne peuvent pas se déduire les uns des autres par des fonctions d'élévation de puissance entière modulo  $n$ , de sorte que le nombre  $A_i$ , et donc l'identité du membre de la liste possédant le certificat  $[A_i, e_i]$  ne peut pas se déduire d'une signature émise par le membre.

15

De préférence, le numéro d'une séquence utilisé pour générer une signature de liste est calculé en fonction d'une date de début de séquence.

20 Avantageusement, la fonction de calcul du numéro d'une séquence est de la forme :

$$F(d) = (H(d))^2 \pmod{n}$$

dans laquelle  $H$  est une fonction de hachage résistante aux collisions,  $d$  est la date de début de la séquence, et  $n$  est un paramètre général de mise en œuvre de la signature de groupe.

25

Selon un mode de réalisation de l'invention, une signature émise par un membre de la liste contient un paramètre qui est calculé en fonction du numéro de séquence et de la clé privée du membre signataire.

30 Selon un mode de réalisation de l'invention, le paramètre  $T_4$  d'une signature émise par un membre de la liste et dépendant du numéro de séquence  $m$  et de la clé privée  $x_i$  du membre signataire est obtenu par la formule suivante :

$$T_4 = m^{x_i} \pmod{n}$$

35  $n$  étant un paramètre général de mise en œuvre de la signature de groupe, et la signature comprenant la preuve que le paramètre  $T_4$  a été calculé avec la clé privée  $x_i$  du membre de la liste qui a émis la signature.

L'invention concerne également un procédé de vote électronique comprenant

une phase d'organisation des élections, au cours de laquelle une autorité organisatrice procède à la génération de paramètres nécessaires à un scrutin, et attribue à des scrutateurs des clés leur permettant de déchiffrer et vérifier des bulletins de vote, une phase d'attribution d'un droit de signature à chacun des  
5 électeurs, une phase de vote au cours de laquelle les électeurs signent un bulletin de vote, et une phase de dépouillement au cours de laquelle les scrutateurs vérifient les bulletins de vote, et calculent le résultat du scrutin en fonction du contenu des bulletins de vote déchiffrés et valides.

Selon l'invention, ce procédé met en œuvre un procédé de signature de liste tel  
10 que défini ci-avant, pour signer les bulletins de vote, chaque électeur étant enregistré comme membre d'une liste, et un numéro de séquence étant généré pour le scrutin, pour détecter si un même électeur a émis ou non plusieurs bulletins de vote pour le scrutin.

15 Selon un mode de réalisation de l'invention, la phase d'organisation comprend la remise à chaque scrutateur d'une clé publique et d'une clé privée, les bulletins de vote étant chiffrés à l'aide d'une clé publique obtenue par le produit des clés publiques respectives de tous les scrutateurs, et la clé privée de déchiffrement correspondante étant obtenue en calculant la somme de clés  
20 privées respectives de tous les scrutateurs.

Avantageusement, le chiffrement des bulletins de vote est effectué à l'aide d'un algorithme de chiffrement probabiliste.

25 Selon un mode de réalisation de l'invention, les bulletins de vote émis par les électeurs sont stockés dans une base de données publique, le résultat de la vérification et du dépouillement de chaque bulletin de vote étant stocké dans la base de données en association avec le bulletin de vote, et la clé privée de déchiffrement des bulletins de vote étant publiée.

30 Un mode de réalisation préféré de l'invention sera décrit ci-après, à titre d'exemple non limitatif, avec référence aux dessins annexés dans lesquels :

35 La figure 1 représente un système permettant la mise en œuvre des procédés de signature de liste et de vote électronique, selon l'invention ;



Les figures 2 à 8 illustrent sous la forme d'organigrammes les différentes procédures qui sont exécutées conformément aux procédés de signature de liste et de vote électronique, selon l'invention.

- 5 La présente invention propose un procédé de signature de liste dans lequel toutes les personnes autorisées, c'est-à-dire appartenant à la liste, peuvent produire une signature qui est anonyme, et n'importe qui est capable de vérifier la validité de la signature sans avoir accès à l'identité du membre de la liste qui a signé.
- 10 Un tel procédé peut être mis en œuvre dans le système représenté sur la figure 1. Ce système comprend des terminaux 2 mis à la disposition des utilisateurs et connectés à un réseau de transmission 5 de données numériques, tel que le réseau Internet. Chaque terminal 2 est avantageusement connecté à un lecteur 8
- 15 de carte à puce 7. Par le réseau 5, les utilisateurs peuvent se connecter à un serveur 6 donnant accès à des informations par exemple stockées dans une base de données 4. Ce système comprend également un calculateur 1 d'une autorité de confiance qui délivre notamment les cartes à puces 7 aux utilisateurs.
- 20 Le procédé de signature de liste selon l'invention reprend dans le procédé de signature de groupe décrit dans le document référencé [1], les procédures suivantes :
- une procédure d'organisation d'une d'un groupe de signataires, qui consiste à
  - 25 mettre en place les différents paramètres et clés publiques nécessaires,
  - une procédure d'enregistrement dans laquelle une personne à inscrire dans le groupe reçoit d'une autorité de confiance un droit de signature, c'est-à-dire une clé privée et un certificat autorisés,
  - une procédure de signature proprement dite au cours de laquelle une
  - 30 personne possédant un droit de signature signe un message, et
  - une procédure de vérification consistant à appliquer un algorithme de vérification à une signature pour vérifier que la signature a été produite par une personne possédant un droit de signature.
- 35 L'invention prévoit en outre une disposition pour garantir l'anonymat d'un signataire, même vis-à-vis d'une autorité de confiance, ainsi qu'une procédure d'organisation d'une séquence consistant à définir un numéro de séquence à

utiliser pour générer des signatures de liste, la vérification d'une signature comprenant en outre une étape de vérification que la signature est unique pour un numéro de séquence donné.

- 5 Le procédé selon l'invention peut également comporter une procédure de révocation, telle que définie dans le document référencé [2]. A l'aide de cette procédure de révocation, une autorité de confiance peut retirer à un membre de la liste, les droits de signature qu'elle lui a précédemment attribués, à partir de l'identité du membre. La mise en place de cette possibilité de révocation
- 10 implique l'exécution par les membres de la liste d'une procédure de mise à jour au cours de laquelle les membres de la liste mettent à jour leurs certificats pour prendre en compte les modifications (ajout ou retractions) effectuées dans la liste des personnes autorisées à signer.
- 15 La figure 2 illustre les différentes étapes de la procédure d'organisation 10 exécutée sur le calculateur 1 de l'autorité de confiance. Conformément au document référencé [1], cette procédure consiste à choisir 11 des nombres entiers suivants :

- 20 -  $\varepsilon > 1$ ,  $k$ ,  $l_p$ ,  
 -  $\lambda_1$ ,  $\lambda_2$ ,  $\gamma_1$ ,  $\gamma_2$  qui sont des longueurs de nombres entiers en nombres de bits, avec :

$$\lambda_2 > 4l_p \quad (1)$$

$$\lambda_1 > \varepsilon(\lambda_2 + k) + 2 \quad (2)$$

25  $\gamma_2 > \lambda_1 + 2 \quad (3)$

$$\gamma_1 > \varepsilon(\gamma_2 + k) + 2 \quad (4)$$

et à définir les ensembles de nombres entiers suivants :

$$\Lambda = ]2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}[ \text{ et }$$

$$\Gamma = ]2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}[.$$

30

Cette procédure consiste également à choisir une fonction de hachage résistante aux collisions  $H$  telle qu'une séquence binaire de longueur quelconque notée  $\{0, 1\}^*$  est transformée en une séquence binaire de longueur  $k$  notée  $\{0, 1\}^k$ .

- 35 Ensuite, le calculateur 1 de l'autorité de confiance génère aléatoirement, à l'étape 12, des nombres premiers  $p'$  et  $q'$  de taille  $l_p$ , tels que  $p = 2p' + 1$  et  $q = 2q' + 1$  sont aussi des nombres premiers. Ensuite, il calcule à l'étape 13 le module  $n = pq$  et génère aléatoirement à l'étape 14 des nombres entiers  $a$ ,  $a_0$ ,  $b$ ,

g et h dans l'ensemble  $QR(n)$  des résidus quadratiques de n, c'est-à-dire l'ensemble des nombres entiers y tels  $y = x^2 \pmod{n}$ , x étant un nombre entier.

On considère alors que la clé publique PK de l'autorité de confiance est constituée de la séquence de nombres entiers (n, a,  $a_0$ , b, g, h) et que la clé  
5 privée de celle-ci est constituée de la séquence de nombres entiers ( $p'$ ,  $q'$ ).

Pour être enregistré par l'autorité de confiance, un utilisateur souhaitant devenir membre de la liste exécute sur son terminal 2 la procédure 20 illustrée sur la figure 3. L'exécution de cette procédure engage un dialogue avec le calculateur  
10 1 de l'autorité de confiance qui exécute alors une procédure 20'. La procédure 20 comprend tout d'abord une étape 21 de génération aléatoire de nombres entiers  $\tilde{x}_i$  et  $\tilde{r}$ , respectivement dans les intervalles  $]0, 2^{\lambda_2}[$  et  $]0, n^2[$ . A partir de ces nombres entiers, on calcule 22 un nombre entier  $C_1$  tel que :

$$C_1 = g^{\tilde{x}_i} h^{\tilde{r}} \pmod{n} \quad (5)$$

15 A l'étape 23, on construit la preuve U de la connaissance de deux nombres  $\alpha$  et  $\beta$  (c'est-à-dire  $\tilde{x}_i$  et  $\tilde{r}$ ) tels que  $C_1 = g^{\alpha} h^{\beta} \pmod{n}$ .

Une telle preuve est par exemple constituée en choisissant aléatoirement deux nombres entiers  $r_1$  et  $r_2$  dans l'ensemble des nombres binaires signés à  $\varepsilon(2l_p + k)$   
20 bits, noté  $\pm\{0, 1\}^{\varepsilon(2l_p + k)}$ , et en calculant les nombres suivants :

$$d_1 = g^{r_1} h^{r_2} \pmod{n}, \quad (6)$$

$$c = H(g \| h \| C_1 \| d_1), \quad (7)$$

dans laquelle le symbole  $\|$  représente l'opérateur de concaténation,

$$s_1 = r_1 - c\alpha, \quad (8)$$

$$25 \quad s_2 = r_2 - c\beta. \quad (9)$$

$s_1$  et  $s_2$  étant des nombres entiers relatifs.

La preuve U est alors égale à (c,  $s_1$ ,  $s_2$ ,  $C_1$ ).

Le nombre  $C_1$  et la preuve U sont ensuite envoyés à l'autorité de confiance qui  
30 vérifie à l'étape 21' la preuve U et que  $C_1$  se trouve dans l'ensemble  $QR(n)$  des résidus quadratiques de n.

Dans l'exemple précédent, la vérification de la preuve U consiste à calculer :

$$t_1 = C_1^c g^{s_1} h^{s_2} \pmod{n}, \text{ et} \quad (10)$$

$$35 \quad c' = H(g \| h \| C_1 \| t_1). \quad (11)$$

La preuve est vérifiée si  $c' = c$  et si  $s_1$  et  $s_2$  appartiennent à l'ensemble  $\pm\{0, 1\}^{\varepsilon(2l_p + k) + 1}$ .

- Si tel est le cas, le calculateur 1 de l'autorité de confiance génère aléatoirement 22' deux nombres entiers  $\alpha_i, \beta_i$  dans l'intervalle  $]0, 2^{\lambda_2}[$ , et envoie ces nombres au terminal 2 de l'utilisateur. Dans la procédure 20, le terminal de l'utilisateur
- 5 calcule alors à l'étape 24 les nombres entiers  $x_i$  et  $C_2$  en appliquant les formules suivantes :

$$x_i = 2^{\lambda_1} + (\alpha_i \tilde{x}_i + \beta_i \pmod{2^{\lambda_2}}), \text{ et} \quad (12)$$

$$C_2 = a^{x_i} \pmod{n}. \quad (13)$$

- 10 Puis, il construit à l'étape 25 les preuves suivantes (par exemple selon le même principe que la preuve U) :

- la preuve V de connaître un nombre  $\alpha$  appartenant à l'ensemble  $\Lambda$  tel que :
 
$$C_2 = a^\alpha \pmod{n} \quad (14)$$

15

- la preuve W de connaître trois nombres  $\beta, \gamma, \delta$  tels que  $\beta \in ]-2^{\lambda_2}, 2^{\lambda_2}[$  et
 
$$C_2/a^{\lambda_2} = a^\beta \text{ et} \quad (15)$$

$$C_1^{\alpha_i} g^{\beta_i} = g^\beta (g^{2^{\lambda_2}})^{\gamma_i} h^\delta \quad (16)$$

- 20  $C_2$  et les preuves V et W sont ensuite envoyés au calculateur 1 de l'autorité de confiance qui vérifie 23' les preuves V et W, et que  $C_2$  appartient à l'ensemble  $QR(n)$ . Si tel est le cas, il génère 24' aléatoirement un nombre premier  $e_i$  appartenant à l'ensemble  $\Gamma$  et applique la formule suivante :

$$A_i = (C_2 a_0)^{1/e_i} \pmod{n} \quad (17)$$

- 25 et renvoie à l'utilisateur les entiers  $A_i$  et  $e_i$  considérés comme un certificat  $[A_i, e_i]$  d'appartenance de l'utilisateur à la liste.

Le calculateur 1 crée 26' alors une nouvelle entrée dans une table des membres de la liste, par exemple dans la base de données 4, dans laquelle il mémorise le certificat  $[A_i, e_i]$  en vue de modifications de la liste (par exemple révocations de

- 30 membres), et de préférence les messages échangés entre l'autorité de confiance et l'utilisateur durant cette procédure d'enregistrement de l'utilisateur.

Par ailleurs, l'utilisateur peut contrôler 26 l'authenticité du certificat reçu en vérifiant que l'équation suivante est satisfaite :

$$35 \quad a^{x_i} a_0 = A_i^{e_i} \pmod{n} \quad (18)$$

A la fin de cette procédure d'enregistrement 20, l'utilisateur dispose donc d'une clé privée  $x_i$  et d'un certificat  $[A_i, e_i]$  de membre de la liste, qui sont par exemple mémorisés dans une carte à puce 7.

- 5 A l'aide d'un tel certificat, l'utilisateur peut générer une signature d'un message  $M$  appartenant à l'ensemble  $\{0, 1\}^*$ .

A cet effet, l'autorité de confiance publie selon l'invention un numéro  $m$  de séquence, choisi aléatoirement dans l'ensemble  $QR(n)$ . Ce numéro devra être utilisé par les membres de la liste pour signer un message durant une séquence

- 10 donnée. Les numéros respectifs de séquences différentes ne doivent pas pouvoir être liés. En particulier, il doit être impossible de calculer un logarithme discret d'un numéro de séquence donné, par rapport à la base d'un autre numéro de séquence, c'est-à-dire qu'il ne doit pas être possible en pratique de calculer des nombres entiers  $x$  et  $y$  tels que :  $m^x = m'^y \pmod{n}$ ,  $m$  et  $m'$  étant des numéros
- 15 de séquence.

Ce numéro  $m$  de séquence peut être calculé en fonction de la date de début de la séquence :  $m = F(\text{date})$ . Cette fonction  $F$  est par exemple choisie égale à :

$$F(d) = (H'(d))^2 \pmod{n} \quad (19)$$

- 20 dans laquelle  $H'$  une fonction de hachage résistante aux collisions, telle qu'une séquence binaire de longueur quelconque notée  $\{0, 1\}^*$  est transformée en une séquence binaire de longueur  $2l_p$  notée  $\{0, 1\}^{2l_p}$ . Il est donc facile de vérifier la validité du numéro de séquence en appliquant la formule (19).

- 25 La procédure de signature d'un message est conçue pour permettre notamment à un utilisateur de démontrer qu'il connaît un certificat de membre et une clé privée de membre et qu'il utilise le bon numéro de séquence.

Pour signer un message  $M$ , un membre de la liste doit exécuter, par exemple sur sa carte à puce 7 connectée à un terminal 2 et mémorisant son certificat  $[A_i, e_i]$

- 30 et sa clé privée  $x_i$ , une procédure 30 de signature, illustrée sur la figure 4. Cette procédure comprend tout d'abord une étape 31 de génération aléatoire d'un nombre  $\omega$  appartenant à l'ensemble  $\{0, 1\}^{2l_p}$ .

Elle comprend en outre une étape 32 consistant à calculer les nombres suivants à partir de  $\omega$  :

35  $T_1 = A_i b^\omega \pmod{n}, \quad (20)$

$$T_2 = g^\omega \pmod{n}, \quad (21)$$

$$T_3 = g^{e_i h^\omega} \pmod{n}. \quad (22)$$

Conformément à l'invention, on calcule également le nombre suivant :

$$T_4 = m^{x_i} \pmod{n} \quad (23)$$

- 5 A l'étape 33 suivante, on génère d'une manière aléatoire les nombres  $r_1$  dans l'ensemble des nombres binaires signés à  $\varepsilon(\gamma_2+k)$  bits, noté  $\pm\{0, 1\}^{\varepsilon(\gamma_2+k)}$ ,  $r_2$  dans l'ensemble  $\pm\{0, 1\}^{\varepsilon(\lambda_2+k)}$ ,  $r_3$  dans l'ensemble  $\pm\{0, 1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$  et  $r_4$  dans l'ensemble  $\pm\{0, 1\}^{\varepsilon(2l_p+k)}$ . Puis, à l'étape 34, on calcule les grandeurs suivantes :

$$d_1 = T_1^{r_1} / (a^{r_2} y^{r_3}) \pmod{n} \quad (24)$$

$$d_2 = T_2^{r_1} / g^{r_3} \pmod{n} \quad (25)$$

$$10 \quad d_3 = g^{r_4} \pmod{n} \quad (26)$$

$$d_4 = g^{r_1} h^{r_4} \pmod{n} \quad (27)$$

Conformément à l'invention, on calcule également le nombre suivant :

$$d_5 = m^{r_2} \pmod{n} \quad (28)$$

- 15 Puis, à l'étape 35, on calcule les nombres suivants :

$$c = H(m \| b \| g \| h \| a_0 \| a \| T_1 \| T_2 \| T_3 \| T_4 \| d_1 \| d_2 \| d_3 \| d_4 \| d_5 \| M), \quad (29)$$

dans laquelle  $\|$  représente l'opération de concaténation,

$$s_1 = r_1 - c(e_i - 2^{\gamma_1}), \quad (30)$$

$$20 \quad s_2 = r_2 - c(x_i - 2^{\lambda_1}), \quad (31)$$

$$s_3 = r_3 - ce_i \omega, \quad (32)$$

$$s_4 = r_2 - c\omega, \quad (33)$$

$s_1, s_2, s_3, s_4$  étant des nombres entiers relatifs.

- 25 La signature est enfin constituée de l'ensemble de nombres suivants :

$$(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3, T_4). \quad (34)$$

qui est par exemple émise par le réseau 5.

- 30 La vérification d'une signature d'un message  $M$  se déroule en exécutant la procédure 40 illustrée sur la figure 5. Cette procédure comprend tout d'abord à l'étape 41, le calcul des nombres suivants :

$$t_1 = a_0^c T_1^{s_1 - c 2^{\gamma_1}} / (a^{s_2 - c 2^{\lambda_1}} b^{s_3}) \pmod{n} \quad (35)$$

$$t_2 = T_2^{s_1 - c 2^{\gamma_1}} / g^{s_3} \pmod{n} \quad (36)$$

$$t_3 = T_2^c g^{s_4} \pmod{n} \quad (37)$$

$$t_4 = T_3^c g^{s_1 - c_2^{y_1}} h^{s_4} \pmod{n} \quad (38)$$

Selon l'invention, elle comprend également le calcul des nombres suivants :

$$t_5 = T_4^c m^{s_2 - c_2^{\lambda_1}} \pmod{n} \quad (39)$$

$$5 \quad c' = H(m || b || g || h || a_0 || a || T_1 || T_2 || T_3 || T_4 || t_1 || t_2 || t_3 || t_4 || t_5 || M) \quad (40)$$

La signature est authentique si les conditions suivantes sont vérifiées à l'étape 42 :

$$c' = c \quad (41)$$

$$10 \quad s_1 \in \pm\{0, 1\}^{e(\gamma_2 + k) + 1}, \quad (42)$$

$$s_2 \in \pm\{0, 1\}^{e(\lambda_2 + k) + 1}, \quad (43)$$

$$s_3 \in \pm\{0, 1\}^{e(\gamma_1 + 2l_p + k + 1) + 1}, \quad (44)$$

$$s_4 \in \pm\{0, 1\}^{e(2l_p + k) + 1}. \quad (45)$$

Si ces conditions ne sont pas vérifiées, la signature n'est pas valable (étape 45).

15

En outre, en accédant à toutes les signatures qui ont été produites pendant une séquence donnée, par exemple dans la base de données 4, on peut vérifier facilement à l'étape 43, à l'aide du paramètre  $T_4$ , si un membre de la liste a signé plusieurs fois : toutes les signatures émises par un membre de la liste comprennent un paramètre  $T_4$  ayant la même valeur pour un numéro de séquence donné.

20

Il est en outre à noter qu'un membre ne peut pas tricher en utilisant une autre valeur car  $T_4$  est fortement lié à  $T_1$ . En effet, la formule de calcul de  $T_1$  peut aussi être écrite de la manière suivante :

$$25 \quad T_1^{e_i} = a_0 a^{x_i} b^{w_{e_i}} \pmod{n} \quad (46)$$

Si  $T_4$  se trouve déjà dans l'ensemble des signatures émises pour un numéro de séquence donné, on en déduit que la signature a déjà été émise par un membre de la liste pour ce numéro de séquence (étape 46).

30

Pour inclure une possibilité de révocation d'un membre de la liste, le procédé qui vient d'être décrit peut être modifié de la manière suivante.

La procédure d'organisation 10 de la liste comprend en outre à l'étape 14, le choix aléatoire d'un nombre  $u$  appartenant à l'ensemble  $QR(n)$ , et la définition de deux ensembles  $E_{add}$  et  $E_{del}$  qui sont initialement vides.

35

La clé publique PK de l'autorité de confiance est alors constituée de la séquence de nombres entiers  $(n, a, a_0, b, g, h, u)$  et des ensembles  $E_{add}$  et  $E_{del}$ .

- 5 Durant la procédure d'enregistrement 20, 20', le calculateur 1 de l'autorité de confiance attribue à l'étape 25' le paramètre  $u_i$  au nouveau membre  $U_i$  de la liste, ce paramètre étant tel que  $u_i = u$ , et met à jour la valeur du paramètre  $u$  en remplaçant cette valeur par  $u^{e_i}$ .

- 10 Le certificat du nouveau membre regroupe alors les entiers  $A_i, e_i$  et  $u_i$ , ce certificat étant mémorisé à l'étape 26' pour des modifications futures et transmis au nouveau membre.

L'autorité de confiance introduit également le nombre  $e_i$  attribué au nouveau membre dans l'ensemble  $E_{add}$ .

- 15 A la réception de son certificat, le nouveau membre vérifie en outre que :  

$$u_i^{e_i} = u \pmod{n} \quad (47)$$

- 20 Les autres membres  $U_j$  de la liste doivent alors exécuter une procédure de mise à jour pour prendre en compte l'arrivée du nouveau membre et donc la modification du paramètre de liste  $u$ . Cette procédure consiste à recalculer leur paramètre  $u_j$  de la manière suivante :

$$u_j = u_j^{e_i} \pmod{n} \quad (48)$$

- 25 De cette manière, la relation (47) est toujours vérifiée pour tous les couples  $(u_j, e_j)$  de tous les membres de la liste.

- La procédure de révocation d'un membre  $U_k$  de la liste dont le certificat est  $(A_k, e_k, u_k)$  consiste pour l'autorité de confiance à modifier le paramètre  $u$  de la manière suivante :

30 
$$u = u^{1/e_k} \pmod{n} \quad (49)$$

et à introduire le paramètre  $e_k$  dans l'ensemble  $E_{del}$ .

- En outre, chaque membre non révoqué  $U_j$  de la liste doit prendre en compte cette révocation (changement du paramètre  $u$ ) en recalculant son paramètre  $u_j$  de la manière suivante :

35 
$$u_j = u_j^b u^a \pmod{n} \quad (50)$$

$a$  et  $b$  étant tels que  $ae_j + be_k = 1$



Pour déterminer a et b, il suffit d'appliquer l'algorithme d'Euclide étendu consistant à effectuer une série de divisions euclidiennes.

- Il est à noter que le membre révoqué (possédant  $e_k$ ) ne peut pas déterminer a et b à l'aide de la formule (50) qui devient  $e_k(a + b) = 1$ , et donc recalculer le paramètre  $u_k$ .

- Durant la procédure 30 de signature par un membre de la liste, il faut en outre à l'étape 31 choisir aléatoirement des nombres  $w_1$ ,  $w_2$  et  $w_3$  de longueur binaire égale à  $2l_p$ , c'est-à-dire appartenant à l'ensemble  $\{0, 1\}^{2l_p}$ , et calculer à l'étape 32 les nombres suivants :

$$T_5 = g^{e_i} h^{w_1} \pmod{n} \quad (51)$$

$$T_6 = u_i h^{w_2} \pmod{n} \quad (52)$$

$$T_7 = g^{w_2} h^{w_3} \pmod{n} \quad (53)$$

15

Il faut aussi à l'étape 33 choisir aléatoirement des nombres  $r_5$ ,  $r_6$ ,  $r_7$  appartenant à l'ensemble  $\pm\{0, 1\}^{e(2l_p+k)}$  et des nombres  $r_8$  et  $r_9$  appartenant à l'ensemble  $\pm\{0, 1\}^{e(\gamma_1+2l_p+k+1)}$ , puis calculer à l'étape 34 les nombres suivants :

$$d_6 = g^{r_1} h^{r_5} \pmod{n} \quad (54)$$

$$d_7 = g^{r_6} h^{r_7} \pmod{n} \quad (55)$$

$$d_6 = T_6^{r_1} / h^{r_8} \pmod{n} \quad (56)$$

$$d_9 = T_7^{r_1} / (g^{r_8} h^{r_9}) \pmod{n} \quad (57)$$

20

Le nombre c inclut alors les éléments suivants :

$$c = H(m \| b \| g \| h \| a_0 \| a \| T_1 \| T_2 \| T_3 \| T_4 \| T_5 \| T_6 \| T_7 \| d_1 \| d_2 \| d_3 \| d_4 \| d_5 \| d_6 \| d_7 \| d_8 \| d_9 \| M) \quad (58)$$

25

Il faut encore calculer à l'étape 35 :

$$s_5 = r_5 - c w_1 \quad (59)$$

$$s_6 = r_6 - c w_2 \quad (60)$$

$$s_7 = r_7 - c w_3 \quad (61)$$

$$s_8 = r_8 - c e_i w_2 \quad (62)$$

$$s_9 = r_9 - c e_i w_3 \quad (63)$$

30

La signature est alors constituée de l'ensemble de nombres suivants :

$$(c, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, T_1, T_2, T_3, T_4, T_5, T_6, T_7). \quad (64)$$

35

La procédure 40 de vérification d'une signature comprend alors en outre le calcul des nombres suivants à l'étape 41 :

$$t_6 = T_5^c g^{s_1 - c 2^{n_1}} h^{s_5} (\text{mod } n) \quad (65)$$

$$5 \quad t_7 = T_7^c g^{s_6} h^{s_7} (\text{mod } n) \quad (66)$$

$$t_8 = u^c T_6^c g^{s_1 - c 2^{n_1}} / h^{s_8} (\text{mod } n) \quad (67)$$

$$t_9 = T_7^{s_1 - c 2^{n_1}} / (g^{s_8} h^{s_9}) (\text{mod } n) \quad (68)$$

$$c' = H(m \| b \| g \| h \| a_0 \| a \| T_1 \| T_2 \| T_3 \| T_4 \| T_5 \| T_6 \| T_7 \| t_1 \| t_2 \| t_3 \| t_4 \| t_5 \| t_6 \| t_7 \| t_8 \| t_9 \| M) \quad (69)$$

- 10 La signature est authentique si les conditions supplémentaires suivantes sont vérifiées à l'étape 42 :

$$s_5 \in \pm \{0, 1\}^{\varepsilon(2l_p + k) + 1}, \quad (70)$$

$$s_6 \in \pm \{0, 1\}^{\varepsilon(2l_p + k) + 1}, \quad (71)$$

$$s_7 \in \pm \{0, 1\}^{\varepsilon(2l_p + k) + 1}, \quad (72)$$

$$15 \quad s_8 \in \pm \{0, 1\}^{\varepsilon(\gamma_1 + 2l_p + k + 1) + 1} \text{ et} \quad (73)$$

$$s_9 \in \pm \{0, 1\}^{\varepsilon(\gamma_1 + 2l_p + k + 1) + 1}. \quad (74)$$

Il est à noter que contrairement à la signature de groupe décrite dans le document [1], il n'est pas possible pour l'autorité de confiance de retrouver l'identité d'un signataire, c'est-à-dire le nombre  $A_i$  du certificat du signataire à partir d'une signature de liste telle que décrite. En effet, contrairement au procédé décrit dans ce document, l'autorité de confiance n'utilise pas une clé privée  $x$  pour générer le paramètre  $b$ , et donc le nombre  $A_i$  ne peut pas être déduit de  $T_1$  et  $T_2$ .

25

En outre, la signature générée par un membre révoqué  $U_k$  sera détectée invalide. En effet, le paramètre  $T_6$  fait intervenir le paramètre  $u_k$  qui a été déterminé à partir du paramètre commun  $u$ , et le paramètre  $t_8$  qui est calculé pour vérifier la signature fait intervenir également le paramètre  $u$  qui a été modifié à la suite de la révocation du membre  $k$ . Il en résulte que, lors de la vérification de signature, les paramètres  $T_6$  et  $t_8$  sont incohérents, et donc que l'égalité entre  $c$  et  $c'$  ne peut pas être vérifiée par la signature du membre  $k$ .

30

Le procédé de signature de liste qui vient d'être décrit peut être appliqué à un procédé de vote électronique. Le procédé de vote électronique selon l'invention

35

comprend plusieurs phases dont l'exécution des procédures du procédé de signature de liste décrit ci-avant.

5 Ce procédé implique l'intervention d'une autorité de confiance 1 organisatrice des élections qui exécute à cet effet une procédure 50 d'organisation du scrutin. Cette procédure consiste à générer les données nécessaires au bon déroulement des élections, une base de données publique accessible à tous dans laquelle sont recueillis les bulletins de vote. Au cours de l'organisation du scrutin, on désigne également des scrutateurs qui vont dépouiller les votes et déterminer le résultat  
10 de l'élection.

L'autorité organisatrice procède tout d'abord à la génération des différents paramètres nécessaires à la mise en place d'une signature de liste, en exécutant la procédure 10 d'organisation d'une signature de liste. Les électeurs doivent  
15 ensuite préalablement s'inscrire, par exemple dans une mairie, sur une liste électorale de manière à recevoir toutes les données nécessaires, à savoir une clé privée  $x_i$  et un certificat  $(A_i, e_i, u_i)$ , pour générer une signature de liste. A l'aide de ces paramètres, les électeurs peuvent participer à toutes les élections futures. Cette procédure d'inscription peut par exemple être exécutée entre une carte à  
20 puce 7 et un terminal 2, la carte à puce mémorisant à la fin de la procédure le certificat de l'électeur.

Avant une élection, l'autorité organisatrice procède à la mise à jour des listes électorales en exécutant la procédure 20, 20' pour les électeurs nouvellement  
25 inscrits, et en enlevant (révoquant) les droits de signature de liste à toutes les personnes rayées des registres électoraux (par exemple les personnes ayant quitté la circonscription ou déchues de leurs droits civiques). Ces révocations sont réalisées en exécutant la procédure de révocation décrite ci-avant. A l'étape 51 de la procédure 50, l'autorité organisatrice publie également un numéro de  
30 séquence  $m$  nécessaire à la mise en place d'une nouvelle séquence de signature de liste, de manière à empêcher les électeurs de voter (signer) deux fois à cette élection.

Par ailleurs, les scrutateurs vont créer 52 les paires de clés publiques/privées  
35 nécessaires, de telle sorte qu'ils doivent tous coopérer pour pouvoir déchiffrer un message chiffré avec la clé publique. A cet effet, le système cryptographique mis en place est choisi de manière à permettre à un électeur de chiffrer un message (bulletin de vote) à l'aide d'au moins une clé publique, tout en

imposant la coopération de tous les scrutateurs pour utiliser la ou les clés privées correspondantes, et ainsi déchiffrer le message.

5 Le partage de la clé privée de déchiffrement entre tous les scrutateurs peut être effectué de la manière suivante.

On considère  $g$  un générateur du groupe cyclique  $G$ . Une clé privée  $x_i$  respective est attribuée à chaque scrutateur  $i$  qui calcule le nombre  $y_i$  appartenant à  $G$  tel que :

10 
$$y_i = g^{x_i} \quad (75)$$

La clé publique  $Y$  à utiliser par les électeurs est obtenue par la formule suivante :

$$Y = \prod_i y_i \quad (76)$$

15 et la clé privée  $X$  correspondante partagée par tous les scrutateurs  $i$  est la suivante :

$$X = \sum_i x_i \quad (77)$$

20 On peut arriver à un résultat analogue en procédant à un chiffrement en utilisant toutes les clés publiques respectives des scrutateurs. Le déchiffrement nécessitant la connaissance de toutes les clés privées correspondantes.

25 Avant d'aller voter, chaque électeur doit mettre à jour son certificat de signature de liste conformément à la procédure de modification décrite ci-avant, à l'aide des paramètres publiés précédemment. Si l'électeur n'est pas radié des listes électorales, cette modification peut être effectuée.

30 Pendant l'ouverture des bureaux de vote, chaque électeur émet un bulletin de vote en exécutant sur un terminal une procédure 60. A l'étape 61, l'électeur sélectionne son vote  $v_i$  et chiffre celui-ci à l'aide de la clé publique des scrutateurs pour obtenir un vote chiffré  $D_i$ . Puis il signe le vote chiffré à l'aide du procédé de signature de liste pour obtenir une signature  $S_i$ . Le bulletin de vote constitué de l'ensemble  $(D_i, S_i)$  du vote et de la signature, est ensuite publié de manière anonyme dans une base de données publique 4.

35 A l'étape 62, le chiffrement du vote est réalisé en utilisant un algorithme de chiffrement probabiliste (c'est-à-dire que la probabilité que deux chiffrements

d'un même message soient identiques est quasiment nulle), tel que par exemple l'algorithme de El Gamal ou de Paillier. Si on applique l'algorithme de El Gamal, le chiffrement est effectué en calculant les nombres suivants :

$$a_j = v_j Y^r \text{ et } b_j = g^r \quad (78)$$

5 dans lesquels  $r$  est un élément aléatoire. Le vote  $v_j$  chiffré est alors constitué par le couple  $D_j = (a_j, b_j)$ . L'électeur  $E_j$  calcule ensuite la signature de liste du vote chiffré  $S_j = \text{Sig}_{\text{liste}}(a_j \| b_j)$ ,  $\text{Sig}_{\text{liste}}$  étant la signature de liste telle que décrite ci-avant, en exécutant la procédure 30 par sa carte à puce 7, laquelle est transmise au terminal 2.

10 L'électeur  $E_j$  a ainsi généré son bulletin de vote  $(D_j, S_j)$  qu'il envoie 64 à la base de données publique 4 au moyen d'un canal de transmission anonyme, c'est-à-dire interdisant de relier un message transmis à l'émetteur de celui-ci. L'électeur peut à cet effet utiliser un terminal public ou un réseau de mélangeurs.

15

A la fin du scrutin, les scrutateurs effectuent le dépouillement du scrutin en exécutant la procédure 70 sur le terminal 3. Cette procédure consiste tout d'abord à générer 71 la clé privée de déchiffrement  $X$  à partir de leurs clés privées respectives  $x_i$  et à l'aide de la formule (77). Puis, à l'étape 72, ils

20 accèdent à la base de données publique 4 des bulletins de vote pour obtenir les bulletins de vote  $(D_i, S_i)$  et pour les déchiffrer.

Le déchiffrement proprement dit des bulletins de vote consiste pour chaque bulletin de vote émis (étape 73) à vérifier 74 la signature  $S_i$  en exécutant la procédure 40 de vérification de signature de liste décrite ci-avant, et si la

25 signature est valable et unique (étape 75), à déchiffrer 76 le vote chiffré  $D_j$  en appliquant la formule suivante :

$$v_j = a_j / b_j^X \quad (79)$$

Les votes  $v_j$  ainsi déchiffrés et vérifiés, avec le résultat de la vérification

30 correspondante sont introduits 77 dans la base de données 4 des bulletins de vote, en association avec le bulletin de vote  $(D_j, S_j)$ .

La clé privée de déchiffrement  $X$  est également publiée pour permettre à tous de vérifier le dépouillement des bulletins de vote.

35 Une fois que tous les bulletins de vote ont été dépouillés, cette procédure 70 calcule à l'étape 78 le résultat de l'élection et met à jour la base de données publique des bulletins de vote en y inscrivant ce résultat, et éventuellement la clé privée de déchiffrement  $X$ .

- Il est aisé de constater que les propriétés énoncées ci-avant, nécessaires à la mise en place d'un système de vote électronique, sont vérifiées par le procédé décrit ci-dessus. En effet, chaque électeur ne peut voter qu'une seule fois
- 5 puisqu'il est facile de retrouver dans la base de données deux signatures émises par un même électeur pour un même scrutin (pour un même numéro de séquence). Dans ce cas, les scrutateurs peuvent ne pas prendre en compte les deux votes ou ne comptabiliser qu'un seul vote s'ils sont identiques.
- Alternativement, on peut prévoir qu'à l'étape 64 d'insertion d'un vote dans la
- 10 base de données 4, on vérifie que le vote émis par l'électeur ne figure pas déjà dans la base de données en y recherchant le paramètre  $T_4$  propre à l'électeur. Si on détecte ainsi que l'électeur a déjà voté pour ce scrutin, le nouveau vote n'est pas inséré dans la base de données 4.
- 15 Ensuite, il n'est pas possible de commencer à dépouiller les bulletins de vote avant la fin du scrutin si au moins un des scrutateurs respecte la règle, puisqu'il faut la présence de tous les scrutateurs pour dépouiller un bulletin de vote. Enfin, le résultat de l'élection est vérifiable par tous puisque les scrutateurs fournissent dans la base de données tous les éléments nécessaires (en particulier
- 20 la clé privée de dépouillement) pour procéder à une telle vérification, et que la vérification d'une signature est accessible à tous en utilisant la clé publique  $PK=(n, a, a_0, b, g, h, u)$  de l'autorité de confiance. Ainsi n'importe qui peut effectuer le dépouillement de la même manière que les scrutateurs et donc s'assurer qu'il a été effectué de manière correcte.
- 25 Les clés des scrutateurs sont bien entendu obsolètes à la fin du scrutin, puisqu'elles sont publiées.

## REVENDICATIONS

## 1. Procédé de signature de liste comprenant au moins :

- 5 – une phase d'organisation (10) consistant pour une autorité de confiance (1) à définir des paramètres de mise en œuvre d'une signature électronique anonyme, dont une clé privée et une clé publique correspondante,
  - 10 – une phase d'enregistrement (20, 20') de personnes dans une liste de membres autorisés à générer une signature électronique propre aux membres de la liste, au cours de laquelle chaque personne (2) à enregistrer calcule (24) une clé privée ( $x_i$ ) à l'aide de paramètres fournis par l'autorité de confiance et de paramètres choisis aléatoirement par la personne à enregistrer, et l'autorité de confiance délivre (25') à chaque personne à enregistrer un certificat ( $[A_i, e_i]$ ) de membre de la liste,
  - 15 – une phase de signature (30) au cours de laquelle un membre de la liste génère (35) et émet (36) une signature propre aux membres de la liste, cette signature étant construite de manière à contenir une preuve que le membre de la liste ayant émis la signature, connaît un certificat ( $[A_i, e_i]$ ) de membre de la liste, et
  - 20 – une phase de vérification (40) de la signature émise comprenant des étapes (41, 42) d'application d'un algorithme prédéfini pour mettre en évidence la preuve que la signature a été émise par une personne en possession d'un certificat de membre de la liste,
- caractérisé en ce qu'il comprend en outre :
- 25 – une phase de définition d'une séquence consistant pour l'autorité de confiance (1) à générer un numéro de séquence (m) à utiliser dans la phase de signature (30), une signature ( $Sig_{liste}$ ) générée durant la phase de signature comprenant un élément de signature ( $T_4$ ) qui est commun à toutes les signatures émises par un même membre de la liste avec un même numéro de séquence et qui contient une preuve que le numéro de séquence (m) a été
  - 30 utilisé pour générer la signature, la phase de vérification (40) comprenant en outre une étape de vérification (43) de la preuve que le numéro de séquence (m) a été utilisé pour générer la signature ;
  - une phase de révocation d'un membre de la liste pour retirer un membre de la liste, au cours de laquelle l'autorité de confiance (1) retire de la liste le
  - 35 membre à retirer et met à jour les paramètres de mise en œuvre de la signature électronique anonyme, pour tenir compte du retrait du membre de la liste ; et
  - une phase de mise à jour des certificats ( $[A_i, e_i]$ ) des membres de la liste pour

tenir compte de modifications de la composition de la liste.

2. Procédé selon la revendication 1,

caractérisé en ce que la phase d'organisation (10) comprend la définition d'un  
 5 paramètre commun (u) dépendant de la composition de la liste, la phase  
 d'enregistrement (20, 20') d'une personne dans la liste comprenant la définition  
 d'un paramètre ( $u_i$ ) propre à la personne à enregistrer qui est calculé en fonction  
 du paramètre (u) dépendant de la composition de la liste et qui est intégré au  
 certificat ( $[A_i, e_i, u_i]$ ) remis à la personne, la phase d'enregistrement (20, 20')  
 10 comprenant une étape de mise à jour du paramètre commun (u) dépendant de la  
 composition de la liste, la phase de révocation d'un membre de la liste  
 comprenant une étape de modification du paramètre commun (u) dépendant de  
 la composition de la liste, pour tenir compte du retrait du membre de la liste, et  
 la phase de mise à jour des certificats des membres de la liste comportant une  
 15 étape de mise à jour du paramètre ( $u_i$ ) propre à chaque membre de la liste pour  
 tenir compte des modifications de la composition de la liste.

3. Procédé selon la revendication 1 ou 2,

caractérisé en ce qu'une signature propre à un membre de la liste et possédant le  
 20 certificat  $[A_i, e_i]$  comprend des paramètres  $T_1, T_2, T_3$  tels que :

$$T_1 = A_i b^\omega \pmod{n},$$

$$T_2 = g^\omega \pmod{n},$$

$$T_3 = g^{e_i h^\omega} \pmod{n},$$

$\omega$  étant un nombre choisi aléatoirement lors de la phase de signature (30), et b,  
 25 g, h et n étant des paramètres généraux de mise en œuvre de la signature de  
 groupe, tels que les paramètres b, g et h ne peuvent pas se déduire les uns des  
 autres par des fonctions d'élévation de puissance entière modulo n, de sorte que  
 le nombre  $A_i$ , et donc l'identité du membre de la liste possédant le certificat  $[A_i,$   
 $e_i]$  ne peut pas se déduire d'une signature émise par le membre.

30

4. Procédé selon l'une des revendications 1 à 3,

caractérisé en ce que le numéro (m) d'une séquence utilisé pour générer une  
 signature de liste est calculé en fonction d'une date de début de séquence.

35

5. Procédé selon la revendication 4,

caractérisé en ce que la fonction de calcul du numéro d'une séquence est de la  
 forme :

$$F(d) = (H(d))^2 \pmod{n}$$



dans laquelle  $H$  est une fonction de hachage résistante aux collisions,  $d$  est la date de début de la séquence, et  $n$  est un paramètre général de mise en œuvre de la signature de groupe.

5                    6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce qu'une signature ( $Sig_{liste}$ ) émise par un membre de la liste contient un paramètre ( $T_4$ ) qui est calculé en fonction du numéro de séquence et de la clé privée ( $x_i$ ) du membre signataire.

10                   7. Procédé selon la revendication 6, caractérisé en ce que le paramètre  $T_4$  d'une signature émise par un membre de la liste et dépendant du numéro de séquence  $m$  et de la clé privée  $x_i$  du membre signataire est obtenu par la formule suivante :

$$T_4 = m^{x_i} \pmod{n}$$

15                    $n$  étant un paramètre général de mise en œuvre de la signature de groupe, et en ce que la signature comprend la preuve que le paramètre  $T_4$  a été calculé avec la clé privée  $x_i$  du membre de la liste qui a émis la signature.

20                   8. Procédé de vote électronique comprenant une phase d'organisation (50) des élections, au cours de laquelle une autorité organisatrice procède à la génération de paramètres nécessaires à un scrutin, et attribue à des scrutateurs des clés leur permettant de déchiffrer et vérifier des bulletins de vote, une phase d'attribution d'un droit de signature à chacun des électeurs, une phase de vote (60) au cours de laquelle les électeurs signent un bulletin de vote, 25 et une phase de dépouillement (70) au cours de laquelle les scrutateurs vérifient les bulletins de vote, et calculent le résultat du scrutin en fonction du contenu des bulletins de vote déchiffrés et valides, caractérisé en ce qu'il met en œuvre un procédé de signature de liste selon l'une des revendications 1 à 7, pour signer les bulletins de vote, chaque électeur étant 30 enregistré comme membre d'une liste, et un numéro de séquence ( $m$ ) étant généré pour le scrutin, pour détecter si un même électeur a émis ou non plusieurs bulletins de vote pour le scrutin.

35                   9. Procédé selon la revendication 8, caractérisé en ce que la phase d'organisation (50) comprend la remise à chaque scrutateur d'une clé publique et d'une clé privée, en ce que les bulletins de vote ( $v_i$ ) sont chiffrés (62) à l'aide d'une clé publique ( $Y$ ) obtenue par le produit des clés publiques ( $y_i$ ) respectives de tous les scrutateurs, et en ce que la clé privée

(X) de déchiffrement correspondante est obtenue en calculant la somme de clés privées ( $x_i$ ) respectives de tous les scrutateurs.

10. Procédé selon la revendication 9,
- 5 caractérisé en ce que le chiffrement (62) des bulletins de vote est effectué à l'aide d'un algorithme de chiffrement probabiliste.

11. Procédé selon l'une des revendications 8 à 10,
- caractérisé en ce que les bulletins de vote émis par les électeurs sont stockés
- 10 dans une base de données publique (4), en ce que le résultat de la vérification et du dépouillement de chaque bulletin de vote est stocké dans la base de données en association avec le bulletin de vote, et en ce que la clé privée (X) de déchiffrement des bulletins de vote est publiée.

1/4

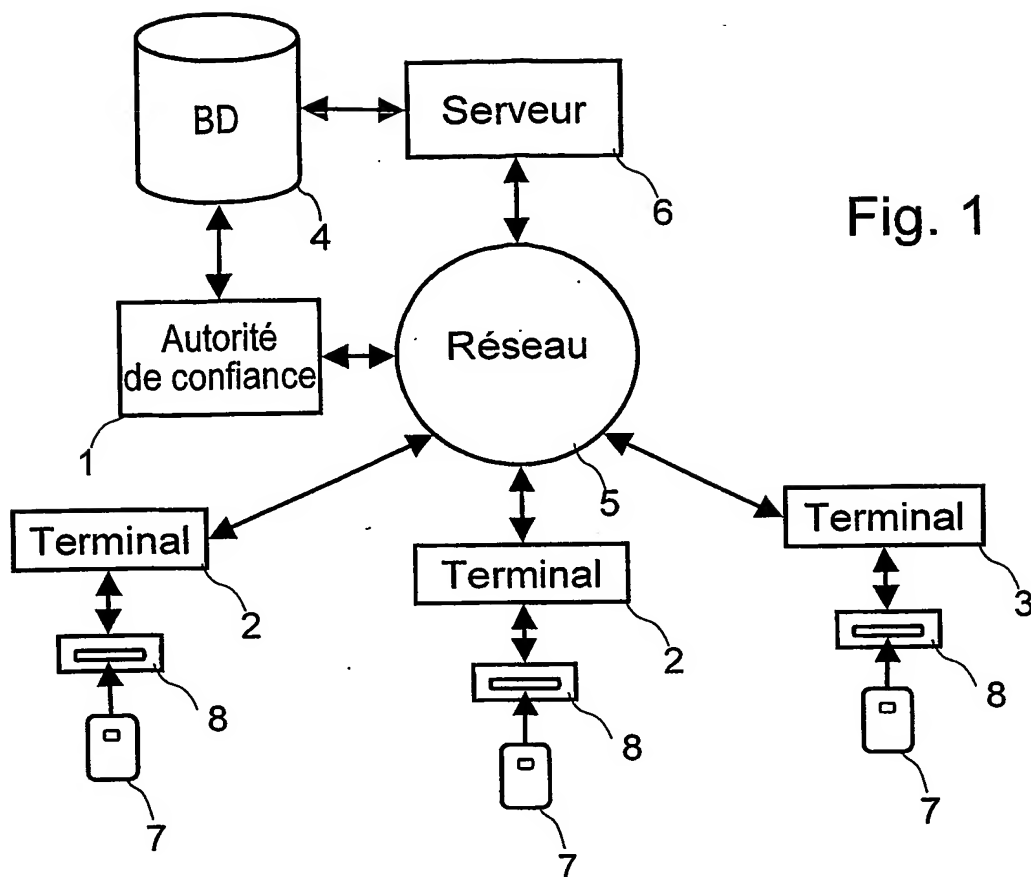
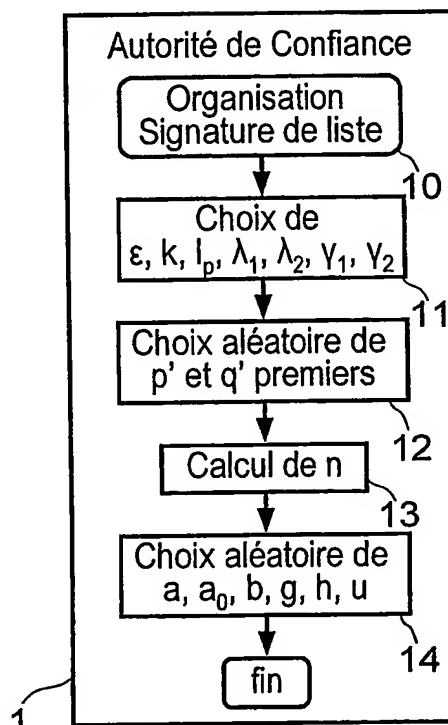
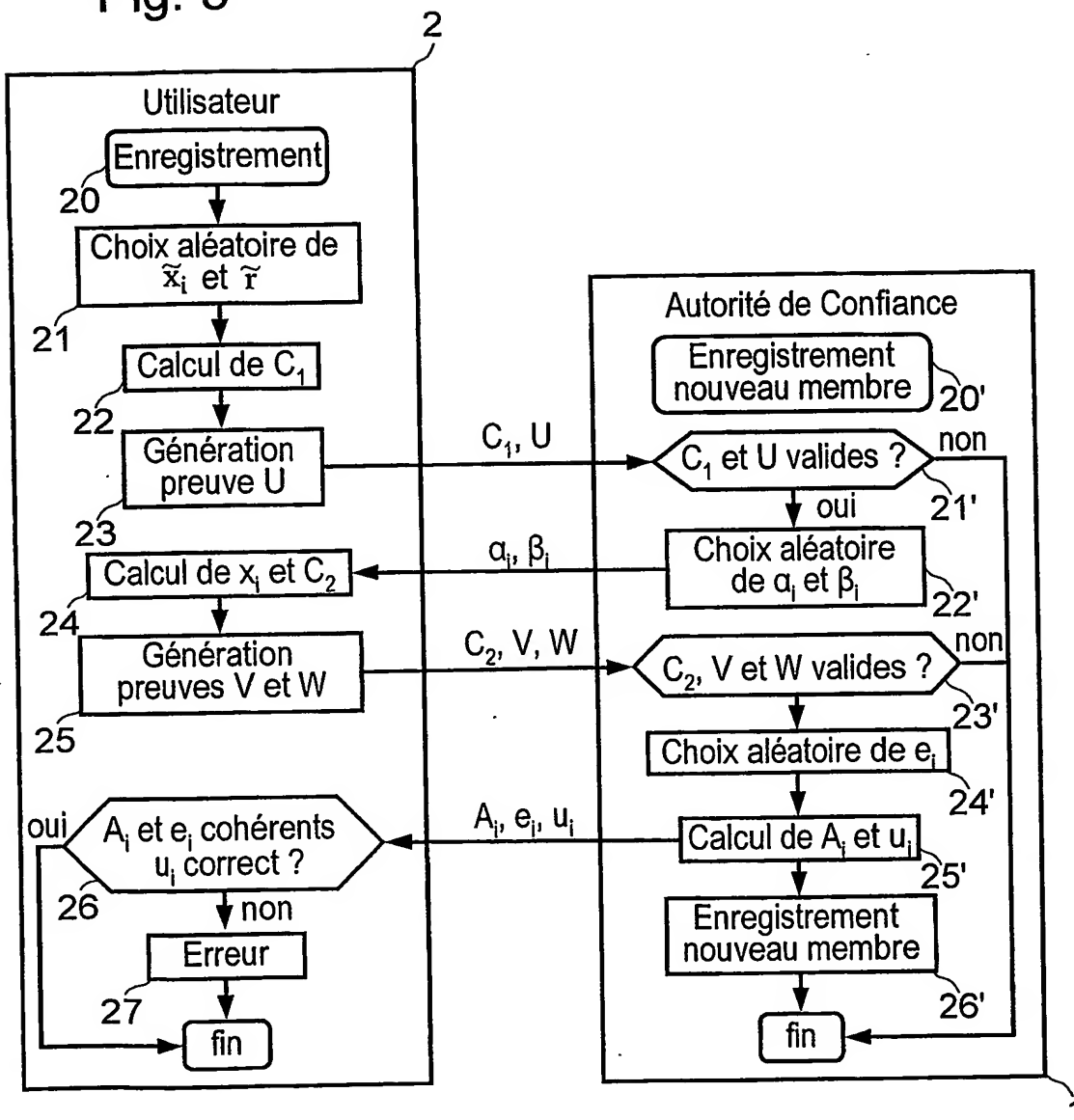


Fig. 2



2/4

Fig. 3



3/4

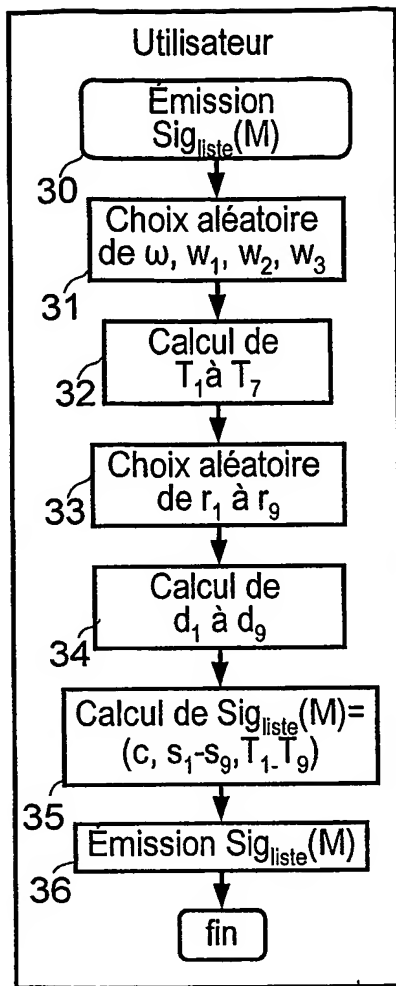


Fig. 4

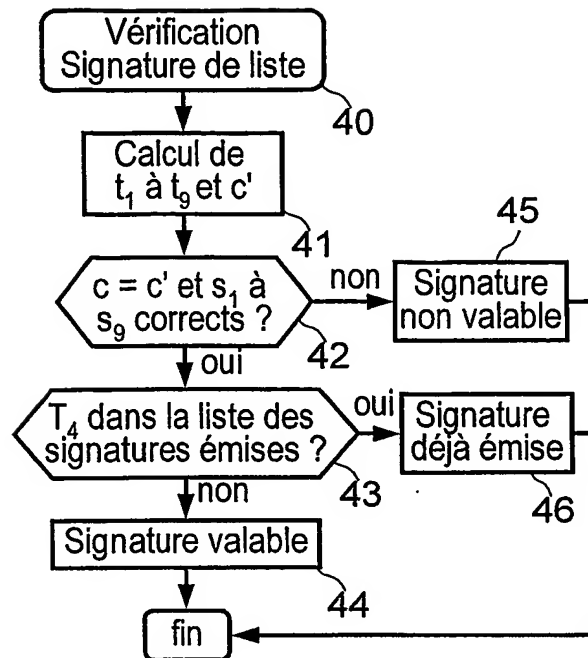


Fig. 5

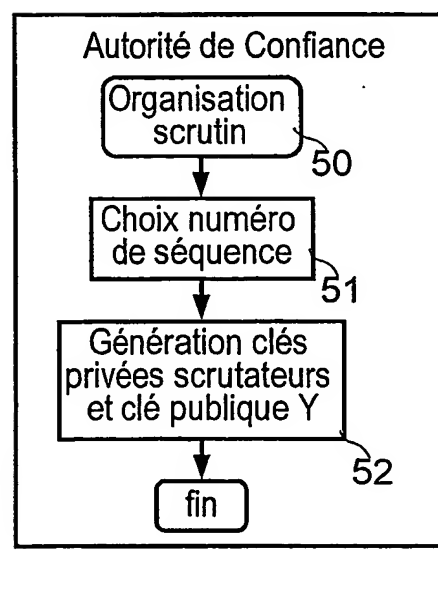


Fig. 6

4/4

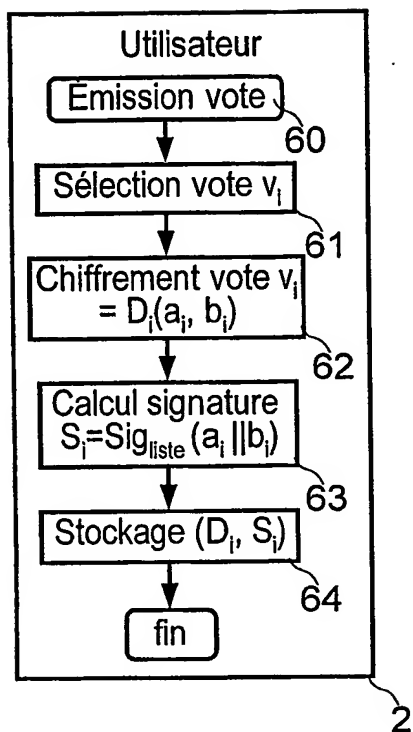


Fig. 7

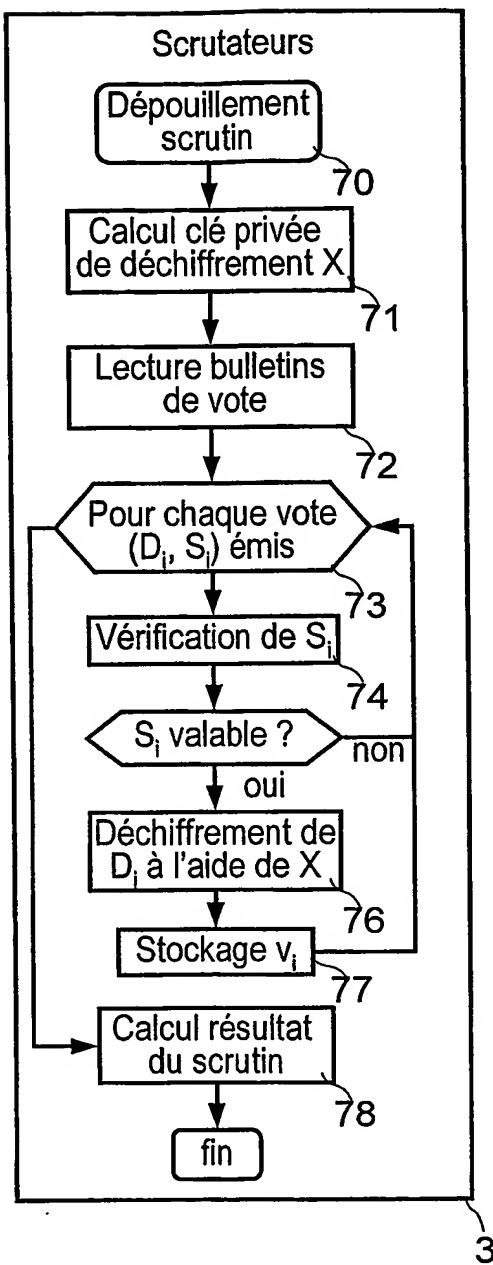


Fig. 8

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 03/02251

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, EPO-Internal, PAJ, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>ATENIESE G ET AL: "A PRACTICAL AND PROVABLY SECURE COALITION-RESISTANT GROUP SIGNATURESCHEME"</p> <p>ADVANCES IN CRYPTOLOGY. CRYPTO 2000. 20TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, AUG. 20 - 24, 2000. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE; VOL. 1880, BERLIN: SPRINGER, DE,</p> <p>20 August 2000 (2000-08-20), pages 255-270, XP001003407</p> <p>ISBN: 3-540-67907-3</p> <p>cited in the application</p> <p>page 262, line 1 -page 263, last line</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/-</p>	1,8

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*G\* document member of the same patent family

Date of the actual completion of the international search

15 December 2003

Date of mailing of the international search report

29/12/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/TR 03/02251

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2001/011351 A1 (SAKO KAZUE) 2 August 2001 (2001-08-02) paragraph '0010! paragraph '0025!	1,8
A	paragraph '0075! - paragraph '0098! paragraph '0101! paragraph '0138! -----	6,7



# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/JP 03/02251

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
US 2001011351	A1	02-08-2001	JP	2001202013 A		27-07-2001
			AU	1639001 A		26-07-2001
			CA	2331991 A1		21-07-2001
			EP	1136927 A2		26-09-2001

---

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 03/02251

## A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

## B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

WPI Data, EPO-Internal, PAJ, INSPEC

## C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>ATENIESE G ET AL: "A PRACTICAL AND PROVABLY SECURE COALITION-RESISTANT GROUP SIGNATURESCHEME" ADVANCES IN CRYPTOLOGY. CRYPTO 2000. 20TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, AUG. 20 - 24, 2000. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1880, BERLIN: SPRINGER, DE, 20 août 2000 (2000-08-20), pages 255-270, XP001003407 ISBN: 3-540-67907-3 cité dans la demande page 262, ligne 1 -page 263, dernière ligne</p> <p style="text-align: center;">--- -/--</p>	1,8

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- \*A\* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- \*E\* document antérieur, mais publié à la date de dépôt international ou après cette date
- \*L\* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- \*O\* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- \*P\* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

\*T\* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

\*X\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

\*Y\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

\*Z\* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 décembre 2003

Date d'expédition du présent rapport de recherche internationale

29/12/2003

Norm et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No  
PCT/FR 03/02251

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 2001/011351 A1 (SAKO KAZUE) 2 août 2001 (2001-08-02) alinéa '0010! alinéa '0025!	1,8
A	alinéa '0075! - alinéa '0098! alinéa '0101! alinéa '0138! -----	6,7

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No

PCT/FR 03/02251

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2001011351 A1	02-08-2001	JP 2001202013 A	27-07-2001
		AU 1639001 A	26-07-2001
		CA 2331991 A1	21-07-2001
		EP 1136927 A2	26-09-2001
<hr/>			